DUDL
NAVA
MONT

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

NETWORK MANAGEMENT
IN AN
EMERGENCY COMMUNICATIONS SYSTEM

by

Richard L. DeLorey Jr.

March 1986

Thesis Advisor: Jack W. LaPatra
CO-advisor: Douglas Moses

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL *(If applicable)*	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS *(City, State, and ZIP Code)* Monterey, California 93943-5100	7b. ADDRESS *(City, State, and ZIP Code)* Monterey, California 93943-5100
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b OFFICE SYMBOL *(If applicable)*	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS *(City, State, and ZIP Code)*	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

11 TITLE *(Include Security Classification)*
ETWORK MANAGEMENT IN AN EMERGENCY COMMUNICATIONS SYSTEM

12 PERSONAL AUTHOR(S)
DeLorey, Richard L., Jr.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT *(Year, Month, Day)*	15 PAGE COUNT
Master's Thesis	FROM Aug. 84 TO Mar. 86	1986 March	60

16 SUPPLEMENTARY NOTATION

17 COSATI CODES		
FIELD	GROUP	SUB-GROUP

18 SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
Network management, monitoring, control strategies, emergency communications requirements

19 ABSTRACT *(Continue on reverse if necessary and identify by block number)*

This thesis begins with a synopsis of contemporary knowledge concerning network management as it has been implemented in a modern communications system, and as it has been postulated by experts in the fields of systems engineering and systems management. It then provides a summary of known operational requirements for a generic emergency communications system, as well as speculation on potential requirements for future application. Finally, it combines the knowledge of network management with the known and projected operational requirements into a proposal for a network management system capable of supporting a generic emergency communications network.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION
☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL	22b TELEPHONE *(Include Area Code)* / 22c OFFICE SYMBOL 54LP

D FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

Approved for public release; distribution is unlimited.

Network Management in an Emergency Communications System

by

Richard L. DeLorey, Jr.
Lieutenant, United States Navy
B.A., Providence College, 1970

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS MANAGEMENT

ABSTRACT

This thesis begins with a synopsis of contemporary knowledge concerning network management as it has been implemented in a modern communications network, and as it has been postulated by experts in the fields of systems engineering and systems management. It then provides a summary of known operational requirements for a generic emergency communications system, as well as speculation on potential requirements for future application. Finally, it combines the knowledge of network management with the known and projected operational requirements into a proposal for a network management system capable of supporting a generic emergency communications network.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

This research was supported, in part, by the National Communications System. In addition, the author acknowledges the contributions of Professors Jack LaPatra and Doug Moses in their roles as Advisor and Co-Advisor, respectively.

I. INTRODUCTION

The availability of reliable communications during an emergency situation is undeniably one of the most critical factors in preventing loss of life, minimizing property damage, and sustaining rescue and recovery operations. However, the broad range of conceivable crises, from local disasters such as floods or tornadoes to situations with national or international impact such as airline accidents or terrorist situations, places extraordinary demands on associated communications systems.

National security-emergency preparedness is the phrase used to describe the ability of our nationwide telecommunications networks to function during times of local or national stress. [Ref. 1: p.15]. In a comprehensive study of national security-emergency preparedness telecommunications policy, Stanford Research Institute International extended the range of possible emergency situations to include a nuclear conflict and concluded that the following six attributes were essential in an emergency communications system: [Ref. 1: pp.122-123]

1. High Network Availability--the likelihood that any given user can gain access to and successfully use the system at a given moment. It includes survivability and restorability in an emergency or war, reliability of individual elements, physical redundancy, particularly in avoiding potentially targeted areas, and a system design responsive to changes in network connectivity.

2. Broad and Controllable Network Access--the need for broad spatial distribution of access points. Defines the ability to control access and then establish a priority call that is maintained across the network.

3. Responsive Network Control--the dynamic allocation of network resources in accordance with prioritized demand. Includes monitoring the condition of network facilities, the status of the overlaying system, and the interfaces with other networks as well as with select users.

4. Extensive Interoperability Among Member Networks--interoperability principally addresses connections between networks that are as transparent as possible

at the user level. It is also important for redundancy through alternate-route networks.

5. Flexible Degree of Dedication--to match the degree of preemption of resources dictated by the magnitude of the situation. Assumes that some sharing of resources is likely and that preemption may apply to both public and private systems. A flexible degree of dedication foresees the time when stored-program controlled facilities can be manipulated by authorized agents to gain needed capability.

6. Wide Range of User Services--refers to user-oriented services with the potential for encryption, and reflects a variety of media such as voice, facsimile, graphics, conferencing, broadcast, and data.

The existence of these attributes in a given communications system is the end-product of a variety of interrelated processes such as planning, design and engineering. However, the degree to which they are successfully implemented to maintain or enhance performance during stressful situations is directly proportional to the degree of efficiency and effectiveness with which network management capabilities are incorporated into network operations. Reflecting the intimate relationship between network management and emergency communications systems, L.A. Gimpelson of ITT's European Headquarters states: "The vital role of a nation's communications network during emergencies is sufficient justification for investment in network management systems" [Ref. 2: p.4]. Lest one is tempted to infer that the intelligence and sophistication of modern communications networks has obviated the requirement for network management, D.G. Haenschke of Bell Laboratories writes: "Telecommunications networks play a vital role during emergencies and natural disasters. The benefits of investments in modern network management capabilities are realized during such emergencies." [Ref. 3: p. 2242]

A. SCOPE

Many discussions of network management are primarily concerned with non-technical organizational and administra-

tive issues such as corporate structure, policy, cost analyses, regulations and legislative affairs, and personnel matters. In yet other presentations, the emphasis is on more technically-oriented subjects such as access, security and traffic flow. While it is true that all of these diverse considerations may be grouped under the heading of network management, they clearly reflect the difference between administrative and operational network characteristics. Therefore, for purposes of this thesis the former category of non-technical, organizational and administrative issues will be labelled external network management, while the latter group which contains technical/operational characteristics of a network or system will be considered as internal network management. Given that distinction, internal network management will be the focal point of this paper, and from this point on will be referred to simply as network management. External management issues, for example the divestiture of AT&T, will be considered insofar as they dictate system requirements or otherwise impact on this discussion, and they will be specifically identified as external management considerations.

B. APPROACH

This thesis will present a synopsis of current literature concerning telecommunications network management and its role in a generic emergency communications network. Depth of discussion and range of considerations were dictated by the topical literature reviewed during the research phase of thesis preparation. Chapter I has provided a general orientation to the subject matter and defined the scope of the thesis. Chapter II will examine the concept of network management in terms of its definition, performance problems which motivate network management initiatives, component functions, and technological capabil-

ities which facilitate modern network management functions. Chapter III is devoted to the network management system in the Bell System's Message Telecommunications Service. In view of their dominant position in the U.S. telecommunications industry it is no surprise that the bulk of available information concerning network management has been generated by the AT&T conglomerate. Then, Chapter IV will outline operational requirements of a generic emergency communications system, and Chapter V will draw together the preceding chapters by proposing a network management system which satisfies the stated requirements of a generic emergency communications system. Finally, Chapter VI will contain general observations, recommendations and concluding remarks.

II. NETWORK MANAGEMENT

The development of direct distance dialing, the proliferation of transoceanic submarine cables, and the advent of satellite communications--all of which occurred during the 1960's--signalled the beginning of the end of manual supervision and control of communications networks. Since that time, dramatic technological advances and an ever-increasing demand for telecommunications services have resulted in the evolution of highly sophisticated, extremely complex telecommunications networks which accomodate a wide variety of devices and offer a broad range of services to the user. However, the size, complexity and technological sophistication of modern networks have created significant network management problems which must be resolved in order to ensure maximum performance of the network under all circumstances. As a result, "Today, in both national and international telecommunications networks, network management has become an indispensable tool for maintaining network integrity and improving network performance during traffic overloads caused by natural disasters, media-stimulated mass callings, equipment failures and traffic surges on major holidays." [Ref. 4: p.157]

Computer technology has undoubtedly been the primary contributor to the numerous advances in communications technology witnessed in recent years. However, it has proven to be somewhat of a double-edged sword. The use of stored-program control and other refinements paved the way for development of automatic routing and automatic controls, and led to increasingly autonomous operations by "intelligent" devices throughout the network. As a result, network management problems have been compounded, particularly in the areas of problem isolation and identification. Thus, in

addition to providing the potential, computer technology has also created the necessity for development of network management systems on a technological par with the networks they are designed to manage. At this point it should be emphasized that despite the strides being made in the field of artificial intelligence and the development of so-called expert systems, no automated system, regardless of its degree of sophistication, is capable of providing optimal response in every situation, nor can it eliminate the need for human intervention in some situations. Therefore, the increasing reliance on automated systems must be tempered with the capacity for manual intervention when required. Wong displays an awareness of this requirement when he writes, "The future approach to network management, both national and international, would be to provide an economical balance between automatic and manual network management capabilities, with emphasis on continued improvement in automatic controls" [Ref. 4: p.158]. A similar attitude is expressed by Westcott, Burruss and Begg who state: "The goal of automated network management is to change the way large computer networks are monitored and controlled in order to allow a more natural form of interaction between human staff and the Network Operations Center" [Ref. 5: p.43].

A. DEFINITION

A concept as broad as network management may be defined or described in many ways. A survey of contemporary topical literature reveals the following examples:

> Successful network management can be succinctly described as the complete, organized control of the motion of data through a network which results in the highest percentage of reliability, availability and utilization with the least amount of internal delay. [Ref. 6: p.819]

> Network management is concerned with network surveillance and control, as well as fault detection and service restoration. [Ref. 7: p.893]

> Network management consists of real-time monitoring and control of the network. It is a technique designed to optimize the capacity of the network when the network is under stress due to traffic overload or failure. [Ref. 3: p.2239]

> Network management can be defined as the function of supervising the network and taking action to control the flow of traffic so as to ensure maximum utilization of the network in all situations. [Ref. 8: p.78]

> The base task of network management consists of monitoring, diagnosis and control. [Ref. 9: p.47]

> The purpose of network management is to optimize the performance of the network during overloads or other stresses. [Ref. 10: p.23]

The common theme of all the above definitions is the employment of monitoring and control functions as a means of optimizing network performance under any conditions, and this common theme provides the basis for a working definition of network management, i.e., network management is the set of monitoring and control functions utilized to sustain and enhance network performance in response to a variety of dynamic operational situations.

B. NETWORK MONITORING

"Network monitoring is the real-time collection and recording of data about network behavior provided by network components" [Ref. 5: p.43]. Its purpose is to give network management an indication of problem conditions in time to initiate corrective actions before network performance is degraded. Simply put, data provided as a result of network monitoring tells management processors and personnel what is happening throughout the network, where problems are developing, and what is the source of the problem. To answer

these questions, several categories of information must be provided, including the status of individual network elements, the overall status of the network, subscriber information and traffic flow data such as offered load and throughput. Obviously, continuous monitoring of a modern communications network would result in generation of massive amounts of data with the potential for overwhelming network management equipment and staff. Therefore, preliminary decisions must be made as to what types of information are required at various levels of the management hierarchy, and how will the information be reported. Determining what types of data are to be reported is a management decision which is based on historical reference data and current system application. However, it normally will involve network configuration, status of network components, or statistical information.

As for how the information will be reported, there are basically three reporting strategies used in modern network management schemes:

1. Automatic reporting--periodic forwarding of information in accordance with a predetermined schedule or on an as-occurring basis.
2. Response reporting--forwarding information in response to polling messages from superior elements in the network, or in response to demands from network management for specific types of information.
3. Reporting by exception--forwarding information on situations which exceeds preset performance standards as promulgated by network management.

The use of response reporting and reporting by exception is one method of controlling the amount of data received at various levels of the management structure. In addition, in most hierarchical management systems a certain amount of filtering and "multiplexing" occurs as data is transmitted upwards through the management hierarchy. Once network monitoring or surveillance processes have reported a failure or alerted network management to an impending problem in the network, corrective or preventive actions must be taken to

maintain network performance levels - hence the need for network control. [Ref. 5: p. 43]

C. NETWORK CONTROL

Network control is the active manipulation/modification of network elements by network management in order to correct, bypass or prevent problems which may detract from overall network performance. The primary problem affecting network performance during an emergency situation is congestion which may be caused by loss of resources or increased demand for service. There are two general types of controls which may be activated to alleviate the impact of congestion on a network: expansive controls and protective controls.

1. Expansive Controls

Expansive controls increase capacity by providing substitute or additional circuit paths for traffic flow to reduce the effects of congestion. Expansive controls improve network performance by utilizing more suitable routing choices during overloads and failures. Since the information required to make decisions concerning alternative routing possibilities is derived from switching systems located throughout the network, the "intelligence" which automates expansive controls is normally located at a central network management location.

2. Protective Controls

Protective controls are also known as restrictive controls and they limit the amount of traffic destined to enter a congested portion of the network, or reduce the number of alternate routing possibilities. The value of protective controls is that during congestion they increase throughput by restricting traffic to the most direct, single link paths. It follows then that the information required for the protective control decision-making process would be available within a given switching system, and therefore the

"intelligence" would be imbedded in the individual switching systems.

In keeping with the previously mentioned desirability of having both automatic and manual control capabilities in a network management system, both expansive and protective controls are capable of being implemented either manually or automatically. Examples of this will be seen in the discussions of specific systems in Chapters III and IV.

D. TECHNOLOGICAL OPPORTUNITIES FOR NETWORK MANAGEMENT

Advanced network capabilities such as stored-program controlled (SPC) exchanges, Common Channel Signalling and dynamic routing provide major opportunities for network management [Ref. 4: p.158].

1. SPC Exchanges

Stored-program controlled exchanges or switching systems employ imbedded computer programs to direct switching operations. Modern SPC exchanges, especially the digital ones, are far more flexible, efficient and powerful than the conventional electro-mechanical exchanges. However, SPC exchanges are susceptible to hardware and software failures which could cause the exchange to fail or congest, thereby putting that portion of the network serviced by the exchange into an overload condition [Ref. 4: p.158].

The most prominent examples of SPC exchanges in modern communications networks are Western Electric Company's No.4 and No.5 Electronic Switching Systems (ESS).

a. No.4 ESS

The No.4 ESS is a high-capacity, toll (Class 4) switching system, and it was the vehicle by which electronic switching was first introduced into the Bell System long distance telecommunications network. No. 4 ESS was designed to provide improved surveillance and control over subordi-

nate portions of the network, and to expand routing opportunities and restrict traffic flow during overload conditions. These features are intended to cope with increasingly complex networks and to maintain overall efficiency of the network despite traffic surges which occur in overloaded portions of the network [Ref. 11: p.1022]. No.4 ESS operations are based upon a high-speed electronic central processor which uses stored-program control to operate the central office on a time-shared basis. In No. 4 ESS, most of the automatic controls,traffic handling, and administrative functions are provided by the stored programs.

b. No. 5 ESS

No. 5 ESS is the first local (Class 5) digital switching system and is the most versatile local/toll switch in the Bell System [Ref. 12: p.258]. No. 5 ESS is similar in design and operation to its toll counterpart, the No. 4 ESS, however, hardware and software advances enable No. 5 ESS to provide more advanced features. No. 5 ESS displays a distributed architecture wherein the system "intelligence" is distributed among the central processor and interface modules located throughout the network. Also, No. 5 ESS offers direct integration with digital transmission systems [Ref. 12: pp.258-259].

> SPC exchanges will become dominant in future telecommunications networks, however special attention should be given to the development of network management techniques that can alleviate switching congestion in an SPC network. [Ref. 4: p.158]

2. Common Channel Signalling

Common channel signalling involves the use of a separate out-of-band channel for carrying set-up and control information between switching systems. In a broader context which is more relevant to this discussion, SPC networks can employ the CCS capability as a high-speed signalling network

separate from, but interactive with, the conventional telecommunications network [Ref. 4: p.158]. By interconnecting SPC exchanges via a CCS network, faster, more reliable and more efficient operation of the network can be achieved. Once again, the most prominent example of CCS technology in operation is found within the Bell System.

a. Common Channel Interoffice Signalling Network

The Common Channel Interoffice Signalling network evolved from CCITT recommendation number 6, and is used to provide reliable, efficient switching capability between SPC exchanges [Ref. 14: p.263]. The CCIS network consists of twenty (20) Signal Transfer Points (STPs) allocated in pairs to each of the ten (10) switching regions across the United States, and the links by which they are connected to the switching systems [Ref. 14: pp.263-264]. Normally the traffic load is shared between the two STPs in each switching region, but each STP is capable of servicing the entire region if its counterpart fails. Links between switching offices and STPs within a region are called A-links and are allocated in pairs--one link to each STP. STPs in a given switching region are connected to all other STPs by B-links which exist in groups of four called quads [Ref. 14: p.264].

3. Dynamic Routing

Dynamic routing is the ability to extend network routing to increase utilization, and is made possible by the use of SPC exchanges communicating via CCS networks. In a dynamic routing scheme, traffic may be routed directly between source and destination exchanges, or it may utilize one or more intermediate exchanges depending upon network conditions. The routing choices between any two exchanges are preset for varying periods of time based on past experience and historical reference data. Dynamic routing implies

a nodal orientation of the network and makes it necessary to place more emphasis on automatic controls that are reliable and robust, and not dependent upon manual administration [Ref. 4: p.158].

Wong also mentions the integrated services digital network (ISDN) as another technological capability amenable to network management. However, ISDN is still in the very preliminary stages of development and does not affect contemporary network management considerations. Having examined network management, its component functions and technological advances which lend themselves to network management efforts, the next step is to look at the problems which create the need for network management in modern communications networks.

E. NETWORK PROBLEMS

Communications networks are required to handle various levels of offered load. However, it is not sufficient to design a system to carry a normal load efficiently and to disregard its performance under overload conditions. In fact, the most widely known aspects of network management are traffic overload controls [Ref. 2: p.4]. Overload conditions occur when the demand for service is greater than network capacity is able to handle efficiently. Increased demand may be generated by natural or man-made disasters, holidays, or events of national interest whereas decreased capacity may result from internal delay or inability to cope with increased traffic load, or the planned or unplanned shutdown of transmission or switching facilities [Ref. 8: pp.79-80]. Haenschke writes that "it is a property of modern telephone networks with common control and alternate routing arrangements that they are highly effective under engineered load conditions but deteriorate under overloads" [Ref. 15: p.1170]. Common control means that one set of

hardware is used to set-up and control the flow of traffic through a part of the network. This is in contrast to nodal-type networks wherein each switching stage is controlled independently throughout a given portion of the network. Modern SPC exchanges are "made-to-order" for a common control approach, and it has become a marked characteristic of modern communications networks. Alternate routing refers to the use of intermediate or substitute circuits when a problem exists in some portion of a network, and is also a characteristic of modern networks [Ref. 8: p. 79].

Under overload, modern networks that employ common control and alternate routing can be forced into an inefficient, congested state marked by a decline in network capacity [Ref. 3: pp. 2240-2241]. There are two basic reasons for the loss of capacity in a network in a congested state: [Ref. 3: pp. 2241-2242]

1. Excessive alternate routing--increases the number of links between source and destination, thereby increasing the amount of blocking which occurs and decreasing the level of network utilization. This situation may be alleviated by restricting the number of alternate routing choices, and by using trunk reservation schemes.

2. Switching delays--the dominant cause of loss of capacity in a network under overload. They may be compounded by user reattempts, and they tend to escalate throughout the network. Network control response depends on both network architecture and switching system(s) architecture.

Excessive or unnecessary application of control measures needlessly inhibits traffic flow, and may create or compound congestion in a network under overload. Therefore, implementation of control responses should be tailored to the existing condition. To support a tailored response, overload conditions are differentiated as follows: [Ref. 2: p. 8-9]

1. General overload--overload which affects the entire network. Within this category fall overloads resulting from increased point-to-point loads throughout the network, and overloads caused by the spread of congestion from a local overload. The best example of a general overload is seen in the telephone

system on occasions such as Christmas or Mother's Day when users throughout the network compete for service.

2. Local overload--overloads caused by small-scale events such as local storms or equipment failures. The response to a local overload is concerned with resolving the existing congestion problem, and perhaps even more importantly, preventing the spread of congestion to other parts of the network. Examples of local overload occur after floods or tornadoes when some users attempt to contact family or friends and yet other users attempt to reach emergency information services, all at the same time.

3. Focused overload--overload caused by abnormally high volumes of traffic into a particular portion of the network. For example, consider a police switchboard at the 911 exchange during an emergency situation. The potential for spread of congestion during a focused overload is very high due to the combination of very low throughput and the very high number of attempts and reattempts by users.

For reasons not entirely clear to the author, discussions in contemporary literature concerning network management and the problems it is intended to alleviate concentrate almost entirely on overload and congestion issues as discussed above. This may indicate that the level of sophistication of modern telecommunications networks is such that other problems are of little or no concern. However, in the examination of emergency communications requirements in Chapter IV, additional network management problems will be identified. Whether or not these problems are unique to emergency communications remains to be seen. In any event, this chapter has provided the background information for the survey of a specific network management system which is presented in the next chapter.

III. THE BELL SYSTEM APPROACH

The heart of the national telecommunications network, and most of its veins and arteries, has been the AT&T Bell System [Ref. 16: p.21]. Since 1909, the stated goal of AT&T has been "one policy, one system, universal service" [Ref. 16: p.21], and during the past seventy five-plus years the goal has become a reality. In conjunction with its operating companies the Bell System became THE telephone company whose standards and specifications are accepted throughout the industry, thus endowing the network with a high degree of interoperability throughout. In addition, visionary planning and continuous refinement of network capabilities and capacity have enabled the network to keep pace with state-of-the-art technology and the ever-increasing demand for services. Having dominated the U.S. telecommunications industry for three-quarters of a century, the Bell System has been the pacesetter in network management, operations and research.

A. MESSAGE TELECOMMUNICATIONS SERVICE

The Message Telecommunications Service (MTS) and the Wide Area Telephone Service (WATS) are the primary components of the Public Switched Network (PSN) and together they comprise the finest long distance telephone network in the world [Ref. 17: pp.17-18]. " The North American Message Telecommunications Service network functions as a single, integrated entity to which customers have access for voice telephone calls, data calls, and other uses such as facsimile transmission" [Ref. 3: p.2240]. At the present time, many initiatives are underway to improve overall management of the MTS including enhanced manual network management controls and real-time network performance

monitoring capabilities. In addition, the network itself is being enhanced by the rapid introduction of Stored-Program Controlled (SPC) exchanges interconnected via the Common Channel Interoffice Signalling (CCIS) system [Ref. 3: pp. 2239-2240].

In the early days of the MTS, each major toll (Class 4) switching system in the network had a dedicated management center which monitored and controlled the performance of only that part of the network serviced by the switching system. More recently, the trend has been towards a "clustered" management approach, i.e., the use of centralized management centers to monitor and control a number of switching systems "clustered" in a large geographical area such as an entire metropolitan area, or in some cases, an entire state [Ref. 3: p. 2246]. As a result, the MTS network management system as it exists today is based on a three-level hierarchy as follows:

Network Operations Center (1)
Regional Operations Center (10)
Network Management Center (27)

1. Network Management Center

The bottom level of the MTS network management hierarchy consists of twenty-seven Network Management Centers, or NMCs, located throughout the United States. Each NMC in conjunction with its supporting operating system provides both automatic and manual capabilities for monitoring performance of the toll (Class 4) and local (Class 5) switching systems within its cluster, identifying actual or potential problems, and initiating appropriate response actions within a time span ranging from a few seconds for automatic controls to a few minutes for manual controls. In addition, the NMC provides the capability for monitoring the performance of automatic controls once they are implemented

and for "fine tuning" the automatic control response as required. The operating system monitors the performance of subordinate portions of the network, collects and forwards performance data, and serves as the medium for implementation of control measures and for transmission of data in both directions between the NMC and other system elements [Ref. 3: pp.2240-2248]. A more in-depth look at the NMC operating system will be presented later in this chapter.

Each Network Management Center is jointly staffed by Bell Operating Company and Long Lines personnel, and in some cases by representatives of independent companies as well. Network managers at the NMC plan the employment of automatic network management controls in the portion of the network under their cognizance. Manual controls are implemented in subordinate switching systems by communicating control commands over the same links used to forward information from the various switching systems [Ref. 3: p.2249].

2. Regional Operations Center

The Regional Operations Center or ROC occupies the middle level of the MTS network management system hierarchy and is supported by the same type of operating system as the NMC. The ROC provides a higher level of performance monitoring and control than is found at the NMC level - whereas the NMC has direct responsibility for the toll (Class 4) and local (Class 5) switching systems within a cluster, the ROC manages the activities of the two or three Network Management Centers in its region. In addition, the ROC may serve as a backup system for its subordinate NMCs in the event of failure at the NMC level. This redundancy is made possible by the fact that both the NMC and the ROC utilize the same operating system. The ROC also has responsibility for first-stage monitoring of the CCIS network in its region [Ref. 3: pp.2247-2248]. There is one Regional Operations Center in each of the ten switching regions delineated by the Bell System throughout the United States.

3. The ROC/NMC Operating System

The operating system which supports activities of both the Network Management Centers and the Regional Operations Centers in the MTS network is called the Engineering and Administrative Data Acquisition System for Network Management (EADAS/NM). There are thirty-one such systems in operation throughout the network with four systems dedicated to supporting four of the ten ROCs, twenty-one systems dedicated to supporting twenty-one of the twenty-seven NMCs, and each of the remaining six systems are shared by a ROC and an NMC, for a total of thirty-one systems.

The primary functions of the EADAS/NM operating system are: [Ref. 3: pp. 2251-2252]

1. Collect network performance data on an event basis every thirty seconds and traffic load data every five minutes. As shall be seen later, these time intervals are preset, and subsequently controlled, at the Network Operations Center.
2. Analyze data to identify "exception" conditions and other less critical performance parameters, and output the results of that analysis to wall displays, printers and CRT terminals in the ROC or NMC.
3. Facilitate activation of network management controls by transmitting control messages to the appropriate switching system(s).
4. Maintain network management databases by auditing and inputting specified performance data. Also allows manual input of data into reference databases.
5. Transmit required information to higher level operating systems to facilitate overall network management.

The local (Class 5) and some small toll (Class 4) switching systems in each NMC cluster are connected with the EADAS/NM system by an intermediate data sub-system simply called the EADAS system. In some cases, the intermediate system may not be Bell's EADAS system, but a similar system provided by an independent company. In time, this situation will probably become more common as a result of the divestiture of AT&T. The larger toll (Class 4) switching systems and the CCIS network's Signal Transfer Points are intercon-

nected with the EADAS/NM system via direct data links which are used to exchange information in both directions [Ref. 3: p.2246].

4. Network Operations Center

The single Network Operations Center (NOC) sits atop the MTS management system hierarchy and is supported by a unique operating system. The NOC is responsible for coordinating and managing the activities of the ten Regional Operations Centers and the twenty-seven Network Management Centers, the international portion of the network which consists of seven gateways through which all overseas traffic flows, and overall management of the CCIS network. The primary objectives of the MTS network management system are:

1. Ensure optimal utilization of network resources,
2. Maximize use of idle capacity when failures occur,
3. Implement control actions as required,
4. Establish a unified network management methodology,
5. Determine the future direction of network management capabilities,
6. Provide guidance to the ROCs and the NMCs regarding control responses to problems in the network, and
7. Conduct network management training.

The centralization of network management responsibility ensures unity of purpose and consistency of application throughout the network. [Ref. 18: pp.2261-2266]

5. Network Operations Center System

The Network Operations Center System (NOCS) is a unique operating system designed specifically to support the Network Operations Center. The basic functions of the NOCS are to collect performance data from subordinate management entities throughout the network at specified time intervals, analyze the collected data, and output the results to graphic displays, printers and terminals in the NOC. Due to

its critical role in the MTS national network management system, an identical system is kept in operational condition at a separate site. Should a failure occur in the on-line system, the back-up system can be brought on-line within fifteen minutes using manual switches to transfer EADAS/NM lines and I/O devices from one system to the other [Ref. 18: p.2268].

Data transfer and message transmissions in both directions between the NOCS and subordinate EADAS/NM systems are accomplished via an intermediate data acquisition system which consists of a Data Transfer Point (DTP) and the links which carry the information. This same intermediate system is used to interface with the seven overseas gateways and the CCIS network's Signal Transfer Points [Ref. 18: pp.2266-2269].

6. System Operations

The two underlying principles of the MTS network management system are polling and exception reporting. As stated earlier, EADAS/NM data collection is performed at thirty second or five minute intervals at both the ROC and the NMC levels depending on the type of information being collected. These intervals are preset at the NOC level and controlled by the NOC operating system's Data Transfer Point. At the start of an interval, the DTP signals both the Network Operations Center System and the EADAS/NM systems. At the lower levels, this signal initiates a polling process whereby messages are sent to subordinate switching systems at the NMC level, and to subordinate EADAS/NM systems as well as subordinate switching systems at the ROC level to elicit forwarding of the required data. At the NMCs, when responses have been received from all "pollees", data analysis is conducted. Exception conditions are identified by comparing collected data with performance thresholds stipulated by the Network Operations Center, and

other performance parameters are isolated as required. The results are output to the various visual, graphic and hard-copy devices in the NMC. In this manner, network managers are alerted to impending problems and kept informed as to the overall status of the network. In addition, information concerning situations which could impact on other portions of the network, and information concerning problems for which control actions have been implemented is transmitted to the ROC. Finally, reference information is input to local databases as dictated by the NMC management staff. At the ROC level, the procedure is basically the same using information provided by the subordinate EADAS/NM systems at the NMC level. At ROCs having the more modern toll (Class4) switching systems within their area of responsibility, additional data is provided by a passive monitoring scheme wherein the data is routinely forwarded from the switching system. This passive monitoring is confined to the more "intelligent" switching systems such as those equipped with SPC technology.

At the Data Transfer Point, incoming data is accumulated until a cutoff point is reached shortly before the end of each interval. At that time, the DTP signals subordinate EADAS/NM systems to cease forwarding information, and transmits the accumulated data the Network Operations Center System. Any information reaching the DTP after this time is discarded. The NOCS performs the same analytical functions as mentioned previously, and outputs results to the various NOC devices and databases. In addition, the NOCS processor stores the data for twenty minutes so that at any given moment, national network management personnel have ready access to data collected during the four most recent intervals.

It should be pointed out that continuous monitoring of the national network results in a tremendous volume of

information being generated. The exception reporting approach used for the majority of data, as well as the filtering/multiplexing of information which occurs at the NMC and ROC levels, prevent the NOCS from being overwhelmed. Also, the majority of control responses are initiated at the Network Management Center level--the lowest level of the system hierarchy. In fact, Haenschke states: "The heart of the MTS network management system is the Network Management Center and its supporting operating system" [Ref. 3: p.2240]. As a result, the bulk of the data which reaches the Network Operations Center at the top of the hierarchy is used for purely administrative purposes such as updating historical databases, setting future performance thresholds, and providing guidance to the ROCs and NMCs regarding application of controls. However, it can be used in a more operational manner to fine tune control responses implemented at lower levels of the network, to resolve problems which are beyond the scope of regional capabilities, or in rare instances to provide backup service in the event of failure at one of the Regional Operations Centers.

The MTS network management system provides a variety of control mechanisms which can be implemented either automatically or manually at any level of the system hierarchy to provide optimal response to changing conditions in the network. The following sections will present a closer look at some of these controls.

B. AUTOMATIC CONTROLS

The increasing "intelligence" of SPC switching systems has been the prime factor in development of a series of automatic network management controls which provide real-time response to existing or impending problems in that portion of the network serviced by the SPC exchange. As mentioned earlier in this paper, these may be either protective or expansive controls.

1. Selective Dynamic Overload Control

Selective Dynamic Overload Control (SDOC) is a protective control used to relieve switch congestion. When a switch becomes congested it sends a signal through the CCIS network to all interconnected switches. Upon receipt of the signal, the other switches respond by reducing the flow of traffic to the congested switch. The reduction in traffic flow may be accomplished by alternate routing, queuing or blocking. This response not only helps reduce traffic to the congested switch, it helps prevent congestion from spreading to other portions of the network [Ref. 10: pp.24-25]. In an SPC network, switching or exchange congestion could be a critical problem. An SDOC response would require that each SPC exchange have the capability of sensing multiple levels of congestion and transmitting overload control signals to other exchanges via the CCIS network. The response to these overload signals would be selective reduction in traffic destined for the congested exchange based on the type of overload signal transmitted. For example, all hard-to-reach traffic (see below) destined for the congested exchange would be restricted at the first level, and at the second level of congestion all that hard-to-reach traffic plus a portion of other traffic destined for the congested exchange would be restricted, and so on. Should the congestion exceed higher levels, more and more traffic destined for the congested exchange would be restricted [Ref. 4: p.159].

2. Hard-To-Reach Traffic

Studies have shown that network congestion due to overload begins with circuit congestion and proceeds to switch or exchange congestion. This transition occurs when successful transmissions which, by definition, involve long holding times on the network, are replaced by numerous unsuccessful attempts which by nature result in short

holding times. The short holding time allows more and more attempts to be made, particularly in an emergency situation, leading to circuit congestion which ultimately creates switch congestion. By blocking unsuccessful attempts, or reducing their number, the congestion could be avoided. Designation of specific destinations as hard-to-reach, based on the volume of unsuccessful attempts, is a means of accomplishing that goal. Because it involves restricting traffic flow to designated destinations, the hard-to-reach measure is a protective control which also enhances the value of other protective controls such as SDOC (see preceding section). Implementation of the hard-to-reach control leaves circuits available for traffic with a higher chance of successfully reaching its destination [Ref. 4: p.159]. Unfortunately, the designation of a specific destination as hard-to-reach is done on the basis of historical reference data. However, the unique nature of emergency situations is such that the necessary data may not be available. Therefore the value of this particular control response in managing an emergency communications network is questionable unless the crisis lasts long enough to allow compilation of requisite reference data.

3. Selective Trunk Reservation

Selective Trunk Reservation (STR) is a protective control that responds to congestion on outgoing circuits or trunks (circuit groups). This control response involves monitoring the number of idle circuits in a trunk, and when that number exceeds a predetermined threshold, the idle circuits are reserved for transmitting traffic for which that circuit or trunk is the first choice route. Since first-choice routed traffic, as opposed to alternate route traffic, normally uses the most direct route between source and destination, the result is higher throughput and therefore more efficient utilization of available network

capacity [Ref. 10: p.25]. In adopting an STR scheme, it would be desirable to use a multiple level approach similar to that described previously in relation to the SDOC mechanism. For example, when the number of idle circuits exceeds the first threshold, the idle circuits would be reserved for all traffic other than hard-to-reach traffic. Then as succeeding thresholds are passed, more and more traffic would be denied access to the reserved circuits [Ref. 4: p.160]. Although the STR scheme is similar in some ways to SDOC, particularly in use of multiple-level responses, it should be noted that while the SDOC response is based on receipt of overload control signals from the congested switch or exchange, the STR response is based on circuit monitoring with no control messages required. The feature that makes both of these protective controls highly effective is that they control hard-to-reach traffic much more severely than other types of traffic [Ref. 3: p.2243].

4. Automatic Rerouting

Sometimes referred to as Automatic Out-of-Chain routing, this expansive control enables traffic which overflowed its normal routing paths to be spread over additional routes that are not normally available for routing. In the Bell System, where it is called Automatic Out-of-Chain routing, up to seven additional routes may be made available. Normally, the additional routes are assigned to each source based on the various destinations. The inherent danger in this control response is that rerouted traffic could end up being "looped" around the network, never reaching its intended destination. Use of a "flag" or classmark will prevent this situation from developing [Ref. 4: p.160]. In the Bell System, Automatic Out-of-Chain routing is made possible by SPC exchanges communicating via the CCIS network. "Automatic Out-of-Chain routing is a first step towards improved network utilization by taking

advantage of capacity often available due to traffic non-coincidence." [Ref. 3: p.2245]

5. Automatic Gapping Control

"Gapping" is a protective control specifically designed to alleviate focused overloads [Ref. 4: p.160]. An example might be the 911 emergency number which is overwhelmed by incoming calls during an emergency situation. Gapping would involve monitoring the number of calls made in a given period of time. When the volume per time interval exceeds a predetermined level, a control signal is transmitted via the CCIS network, and all interconnected switches respond by blocking traffic to that destination for a specified "gap" period. When the gap time has passed, waiting traffic would be forwarded one at a time, with the same gap period between each one, until the overload situation has been resolved. Resolution of the overload would be indicated to the various switches by another control message transmitted via the CCIS network.

C. MANUAL CONTROLS

Manual controls are extremely desirable in modern network management systems to respond to situations beyond the scope of automatic controls, to "fine tune" automatic control responses, and to provide a backup capability in the event of hardware or software failure that affects automatic controls. Wong provides comments on several types of manual controls as follows: [Ref. 4: p.160]

1. Circuit Group Controls

This category of manual controls should include manual rerouting to assign traffic to routes not normally available, manual cancellation of direct or alternate routes to/from a particular circuit group, and manual skip control which causes traffic to "skip over" or bypass a trunk in the normal routing chain. It should be fairly obvious that manual routing and manual cancellation controls are anala-

gous to the automatic alternate routing (AOOC) and Selective Trunk Reservation (STR) controls, respectively. "In all manual circuit group controls, network managers should be able to specify the percentage of traffic to be affected and the type(s) of traffic to be affected. This would allow network problems to be resolved by controlling a minimum of traffic and not by over-controlling." [Ref. 4: p.160]

2. Manual Code Controls

Manual code controls are similar to automatic gapping controls except that they are initiated manually. At each switch or exchange, network managers should be able to specify controlled destinations, gapping intervals, and duration of the controls.

3. Automatic Control Modifications

When automatic controls are triggered, network managers should be able to "fine tune" or adjust their parameters in order to provide optimal response to the problem at hand. This is particularly true in emergency situations since each crisis is fairly unique unto itself, and therefore automatic controls may not provide the optimum response. The parameters to be modified might include response levels in the STR and SDOC functions, or standards for designating a particular destination as hard-to-reach. "Since the optimum control response depends on the severity, geographical distribution and type of overload, maximizing network performance requires the coordination of automatic control responses with manual controls employed in combination." [Ref. 19: p.382] Table I below illustrates the relationship between automatic and manual control responses relative to a particular network problem

The preceding overview of the MTS network management system indicates that it contains the capabilities necessary to achieve optimal performance of the network under a

TABLE I

AUTOMATIC VS. MANUAL CONTROLS

Network Problem	Automatic Control Response	Manual Control Response
Switching Congestion	SDOC	None
Trunk Congestion	STR	Cancellation/ Skipping
Route Deficiency	AOOC	Rerouting
Focused Overload	Gapping	Code Controls

variety of operational circumstances. Its applicability to a generic emergency communications system will be considered later, but in view of the structure and capabilities of the managed network, it is obvious that this particular network management system will be a primary consideration in the network management system proposed in Chapter V.

IV. EMERGENCY SYSTEM REQUIREMENTS

Under normal circumstances, the goal of network management is to provide maximum performance in response to user demand. Technically, this is accomplished by minimizing the amount of blocking which occurs in the network, thereby maximizing the level of call completion. The primary cause of blocking in a network is congestion which may be generated as a result of overload or failure in some portion of the network. This explains the concern with avoiding and/or preventing congestion which was so obvious in the Message Telecommunications Service network management system discussed in the previous chapter of this paper. However, in an emergency situation, the priorities are significantly altered. In fact, in order to support emergency communications during a crisis, it is necessary to restrict or block communications other than those originated by designated critical users. Therefore, the role of network management is altered as well. Performance is still the main concern, but it is performance strictly defined in terms of designated users, precedence, and available network resources. This chapter examines several operational capabilities which would enable a network management system to support critical user communications during an emergency situation by controlling user access, identifying and preserving traffic precedence levels, and optimizing utilization of available network resources and capacity.

A. SURVIVABILITY

Survivability of a communications network is defined as the ability of the network to provide service to critical users during stressful situations. The concerns embodied in the survivability issue are physical destruction of network

facilities, and traffic load in excess of the network's designed "worst-case" capability [Ref. 20: p.103]. Survivability is clearly the most fundamental requirement of an emergency communications system, and it is a function of both availability and connectivity. Availability refers to the ability of users to access the network despite the loss of some network components, and it implies a broad distribution of access points throughout the network. Connectivity concerns the ability of one site to communicate with other sites remaining in the network. These are not independent functions, for access is meaningless without the ability to establish communications, and vice versa [Ref. 20: p.105].

There are many approaches taken when considering network survivability, but the basic choice is between protection and proliferation [Ref. 21: p.169]. The protection viewpoint is that the system can be physically protected from damage through such measures as "hardening" of network facilities and equipment, and electromagnetic pulse (EMP) shielding. On the other hand, the proliferation approach reflects the theory that distribution of functions and capabilities at numerous locations throughout the network ensures that a significant percentage of those network functions and capabilities will remain intact. Of the two, proliferation appears to be the most feasible, for the following reasons:

1. In terms of both time and money, proliferation is less costly than hardening [Ref. 21].
2. Due to those costs, hardening can be accomplished only at a limited number of locations in the network. Therefore, choices must be made as to which sites will be hardened, and the variables involved in that decision-making process are "best guess" estimates at most. For example, if the decision to harden a given site is based on the probability that that particular site will be a target during a war, as opposed to another site, the survivability of that site depends on the validity of the targetting estimate, and the degree to which hardening that is accomplished can withstand the various types of possible enemy strikes.
3. Using a proliferation approach, survival of the network's communications capability is not dependent upon survival of specific portions of the network.

4. The proliferation approach is highly compatible with network management functions, and promotes full utilization of network management capabilities in support of the survivability objective.

With regard to network management functions, the proliferation approach dictates wide distribution of both monitoring and control capabilities throughout the network. Should portions of the network be lost, the redundancy of these capabilities ensures back-up services that will allow monitoring and control functions to continue in surviving portions of the network. Also, redundancy of access points throughout the network ensures that critical users will be able to utilize remaining communications resources. As far as connectivity is concerned, the application of network management controls aids in taking maximum advantage of surviving communications resources and capacity. More specifically, restrictive measures will control the flow of traffic to avoid overwhelming available resources and to increase the potential for use of the network by critical users. In addition, expansive controls provide increased potential for connectivity in support of critical user communications.

The concept of critical users figures prominently in the preceding discussion of survivability, and is the basis for implementation of precedence-related functions in a network management system that supports emergency communications. Designation of critical users is an external management function, and as such is beyond the scope of this discussion. However, SRI concludes that there is a definite need for a coordinated effort in this area among a variety of associated organizations including the National Communications System, the Federal Communications Commission, and the Federal Emergency Management Agency [Ref. 1].

B. ACCESS CONTROL

As noted in the previous section, broad distribution of access points throughout the network is a prerequisite for achieving availability, and therefore survivability, when the proliferation approach is adopted. However, in view of the normal public reaction to an emergency situation, it is to be expected that the demand for access will be excessively high, and so a control problem will be created that must be resolved in order to support emergency communications by critical users. Once critical users have been identified at the various levels of government and industry, priorities must be established among them, and a mechanism for providing requisite services to those users must be implemented.

Network recognition of designated critical users can be accomplished by maintaining reference databases with pertinent information at each access point throughout the network. A code or other type of identification data would be entered when attempting to gain access to the network. The network management system would compare the identification data with the reference table to confirm the critical user designation, and then grant access to the network. Once access is obtained, a variety of functions can be employed to support critical user communications. In recognition of varying priorities among critical users, a multi-level precedence preemption capability can be implemented, similar to those found in the AUTOVON and AUTODIN systems used in the military world. Multi-level precedence preemption (MLPP) allows critical users to obtain access to available circuitry in preference to other users, and if all circuits are in use, the higher precedence of a given user may force lower precedence users to relinquish circuits required to effect the higher precedence communications, even at the expense of ongoing communications [Ref. 22:

p.26]. A further refinement would be installation of an audible or visual alarm system to indicate incoming, high precedence traffic. The use of flags or classmarks reflecting precedence levels would trigger both the preemption and alarm functions as appropriate.

To further enhance performance of surviving portions of the network, existing management controls can be modified and applied as required. For example, selective trunk reservation can be accomplished on the basis of precedence levels rather than offered load to improve delivery of critical user traffic. Also, the use of expansive controls would increase the options for alternate routing and allow tailoring according to traffic priority and user precedence.

C. INTEROPERABILITY

The abundance of public and private communications networks throughout the nation provides ample opportunity for integration and redundancy of network resources in an emergency communications system. The underlying philosophy is that "the more ubiquitous and interconnected a network is, the more difficult it would be to destroy its connectivity" [Ref. 23: p.1]. By interconnecting a variety of networks, the survivability of the composite whole will be greater than the individual survivability of its component parts. This concept is examined in a study performed for the Defense Nuclear Agency by SRI, which includes a proposal for an aggregate system called USNET (Ubiquitous Survivable Network) [Ref. 23]. The USNET concept integrates various networks through the use of intelligent devices called gateways which provide the interface and switching functions required to route traffic between distinct networks. Depending on the physical separation between the networks to be interconnected, the gateway will be characterized as either centralized or distributed. A centralized gateway connects individual networks by direct physical attachment

such as a cable or optical fiber, and imbedded software programs perform required format translations and other interface requirements. The distributed gateway is actually a "mini" communications link between the networks to be interconnected and interface requirements can be satisfied at either end of the gateway link [Ref. 23: pp.93-95]. The gateway function is accomplished using computer technology and can be imbedded in intelligent switching systems such as SPC exchanges. In addition to enhancing survivability, the ability to interconnect distinct networks increases the options for alternate routing, thereby contributing to the success of critical user communications.

D. RESPONSIVE NETWORK MANAGEMENT CONTROLS

The use of network management controls in support of an emergency communications system is a prime factor in sustaining connectivity among surviving portions of the network, and in maximizing utilization of available capacity. The distribution of intelligent switching systems with imbedded automatic control capabilities ensures that a modicum of control can be exerted on surviving portions of the network. In addition, management centers with manual control capabilities should be distributed throughout the network to provide more optimal control response to changing network conditions. As discussed in Chapter II of this paper, control functions are one of the two basic components of network management systems. To effectively support an emergency communications system, the following controls should be implemented with the option of either automatic or manual activation:

1. Access Control--performs the functions discussed earlier in order to guarantee availability of surviving network resources to designated critical users, and to activate control actions which support critical user communications, such as precedence routing.

2. Alternate Routing--perhaps the most important control function to be activated in an emergency situation, the ability of surviving network elements to select

the best path for routing emergency traffic is essential in sustaining connectivity and maximizing utilization of available capacity.

3. Selective Reservation--the ability to reserve circuits for specific types of traffic, particularly on the basis of precedence levels.

In addition,other restrictive and expansive controls may be initiated as required by the situation at hand.

E. DISTRIBUTED NETWORK MONITORING

Acquisition and reporting of status, configuration and performance data is essential to establishing emergency communications, restoring damaged portions of the network, and gradually reconstituting the entire communications network. Monitoring of subordinate portions of the network by intelligent network devices should be supplemented by a remote monitoring capability at selected locations throughout the network. In addition, reporting of required data should be able to be performed both horizontally and vertically to reduce the impact of the loss of superior elements in the network management hierarchy. If the next higher element which normally receives data is destroyed or cannot be reached, pertinent data can be communicated laterally through peer elements until a path to a higher level element is reached. The availability of timely and accurate data regarding conditions throughout the network determines the effectiveness of control responses since those responses are made on the basis of available information.

Successful implementation of the five characteristics discussed above will result in an emergency communications system that displays most of the essential attributes as defined by SRI. It must be emphasized, however, that this discussion is concerned with the role of a network management system, and there are many external considerations to be taken into account when developing an emergency communications system. Also it should be remembered that while the characteristics above are categorized as network management

functions, their effectiveness can be enhanced by other factors such as hardening and EMP shielding, mobility or concealment.

V. A MANAGEMENT SYSTEM PROPOSAL

The following proposal for a network management system is applicable to a generic emergency communications system. A "black-box" approach is used wherein the "what" and not the "how to" is considered. In addition, the underlying assumption is that to minimize the impact of constraining factors such as time and money, existing resources will be used to the greatest extent that is practicable. The intention is to develop a system that satisfies the requirements defined in the preceding chapter, and is, therefore, capable of supporting an emergency communications system regardless of the nature of the emergency, its scope, or its impact.

The generic emergency communications system consists of the Public Telephone Network and a variety of supplemental networks from the public and private sectors. Network switching systems utilize state-of-the-art technology and fall into five classes:

- Regional (Class 1)
- Sectional (Class 2)
- Local Area (Class 3)
- Toll (Class 4)
- End Office (Class 5)

These classes are analagous to the classification currently used in the Bell System with the exception of the Class 3 switches. The local area designation at the Class 3 level is used in deference to the definition of Local Access and Transport Areas (LATA) in Bell's implementation plan for the modified final judgement in the antitrust suit. In addition, the proliferation theory indicates that lower level switches, i.e., Class 4 and Class 5, are more likely to survive in most emergency situations due to their significantly greater number and wider distribution throughout the

network. For this reason, the lower level switches will be key components of the proposed network management system.

A. PROPOSED ARCHITECTURE

The proposed network management system is based on a four-level hierarchy structured as follows:

National Management Center (1)
Area Management Centers (3)
Regional Management Centers (10)
Local Management Centers (30)

1. National Management Center

The National Management Center sits atop the proposed network management system and has overall responsibility for operation of the entire emergency network. Its basic objectives are the same as those of the Bell System's Network Operations Center (see Chapter III). Therefore, National Management Center operations during an actual emergency situation consist of monitoring the status of those portions of the system which survived, providing guidance to lower-level management facilities as required to ensure optimal use of exisiting resources, and to resolve network problems which transcend the capabilities of the Area Management Centers. In addition, the National Management Center is capable of assuming the responsibilities of any one, two, or all three of the Area Management Centers in the event of failure or destruction. The National Management Center itself is "backed up" by the three Area Management Centers which are described in the next section. Should the National Center fail or be destroyed, overall system responsibility is assumed by one of the Area Centers, in accordance with pre-established policy guidelines. As will be seen in the next section, each Area Center maintains national databases, and therefore, the assumption of national responsibility poses no transitional problems.

2. Area Management Centers

The Area Management Centers occupy the next highest level of the proposed hierarchy and are responsible for managing and coordinating the operations of the regional and local management centers within their respective areas of responsibility. The areas of responsibility are defined by dividing the United States into three geographic areas arbitrarily labelled as the Eastern, Mid-American and Western operating areas. In addition, each of the Area Management Centers has the capability of assuming the responsibilities of either one, or both, of the other Area Centers. This requires horizontal as well as vertical communications capabilities, and the ability to terminate circuits from the ten Regional Management Centers in each of the Area Centers. In addition, each of the Area Management Centers must maintain complete national databases to support the backup capability. Furthermore, in the event that the National Management Center fails, or is destroyed, overall responsibility for the emergency system shifts to one of the Area Centers according to a predetermined "line of succession".

3. Regional Management Centers

The ten Regional Management Centers reflect the Bell System's ten switching regions which encompass the entire nation. Each Regional Center is responsible for monitoring and controlling activities of the subordinate local management centers, and is capable of assuming their responsibilities in the event of failure. In addition, each Regional Center is capable of assuming the operational responsibilities of two of the adjacent Regional Centers at one time.

4. Local Management Centers

Although they occupy the lowest level of the proposed management system hierarchy, the Local Centers are the most critical elements of the system. It is at this level that the bulk of the monitoring and control functions

are performed. The Local Centers are responsible for monitoring and controlling subordinate portions of the network. The total of thirty Local Centers results from the allocation of three within each of the ten switching regions.

B. SYSTEM OPERATIONS

The proposed network management system normally exists in a standby mode where the component network elements conduct "business as usual" until emergency conditions are declared. At that point in time, appropriate signals are transmitted through the management hierarchy to activate emergency mechanisms including access controls, horizontal communications capabilities between management centers, and increased reporting periodicities. The lower level network elements continue monitoring subordinate portions of the network, and forward reports in response to polling messages from higher level network components. If no polling messages are received within a predetermined time span, reports are automatically forwarded to designated alternate local centers. At the local management centers, an overall assessment of network conditions is gradually constructed on the basis of incoming data. The absence of data is also significant for if reports are not received from specific network elements within established time intervals, those elements are assumed to have failed. Appropriate information is also forwarded to the next higher level management center where the same process takes place. Gradually, each surviving management center obtains a picture of conditions in the subordinate portions of the network, and determines what remedial actions should be taken.

As communications are attempted, user identification data is compared with reference tables to confirm designation as a critical user, and to determine the appropriate precedence for that critical user. If the comparison results are negative, the call is terminated. If the desig-

nation is confirmed, access is granted with traffic flagged appropriately to trigger precedence-based control mechanisms which support the critical user communications. If conditions warrant, selected circuits will be reserved for specific types of traffic as long as demand exists. If these reserved circuits become idle beyond established thresholds, they will be released for other types of traffic. As traffic is routed through surviving portions of the network, monitoring data is utilized at each switching point to determine the best route to use for the next link in the communications path. This may involve use of another network. In this case, traffic is routed to the appropriate gateway where format translation and other interface requirements are performed, and that network serves as the next link in the communications chain. Additional restrictive and/or expansive controls are implemented as dictated by the situation at hand.

At surviving regional and national management centers, network status and configuration as well as traffic load are monitored closely, and control responses initiated at lower levels are adjusted as required to obtain optimal performance and response. As incoming data indicates that damaged portions of the network have been restored, this information is transmitted through the network so databases may be updated, and monitoring and control functions can be adjusted accordingly. In this manner, restored portions of the network are brought back into service, capacity is increased, the level of service to users is increased, and gradually full service operations are restored. As the network is gradually reconstituted, control measures are relaxed accordingly, and access is granted to an ever-increasing segment of the affected population.

Obviously, this proposed network management system closely resembles the network management system implemented

in the Bell System's Message Telecommunications Service as discussed in Chapter III. Given ATC years of experience and accumulated expertise, it is not surprising that their operational system offers the majority of functions and capabilities desired in a network management system capable of supporting an emergency communications system. Modifications to the MTS network management system incorporated into the proposed system are as follows:

1. Greater redundancy of management facilities at the national and local levels to increase survivability.
2. Establishment of Area Management Centers at the second level of the proposed management system hierarchy to enhance control of the network during a crisis, and to provide back-up services should the National Management Center capabilities be lost.
3. Distribution of Class 3 switches on the basis of LATAs as defined in the implementation plan for the modified final judgement to lessen the long term impacts of divestiture.
4. Lateral reporting capabilities at each level of the network management hierarchy to facilitate redundancy of network components and provision of back-up services at peer levels.
5. Inclusion of access controls and other precedence-based control functions to support critical user communications.

The proposed management system uses a proliferation approach to cope with the impacts of an emergency situation. However, like the emergency communications system itself, the effectiveness of the proposed network management system will be enhanced by hardening of facilities and other external procedures which may be initiated.

VI. SUMMARY

The focal point of this thesis has been internal network management and its role in supporting a generic emergency communications system. In addition a proposed network management system for a generic emergency communications system was described, and proved to be very closely related to the network management system implemented in support of the Bell System's Message Telecommunications Service. Not only does this reflect ATC overwhelming experience and expertise in the area of network management, but it leads to the conclusion that the major problems in actually fielding an effective network management system to support emergency communications requirements are not internal network management problems. The technical capabilities and the necessary resources for developing and implementing an effective network management system to support emergency communications are readily available. With relatively minor modifications, the same system used in day-to-day operations is more than capable of functioning with equal efficiency and effectiveness in an emergency situation. In this context, the following recommendations are offered for consideration:

1. Increase distribution of network management facilities to provide greater redundancy in monitoring and manual control capabilities.
2. Accelerate conversion of remaining electromechanical switches to modern SPC switching systems to maintain control as low as possible in the hierarchy, and therefore with as wide a distribution as possible.
3. Develop an increased capability for remote monitoring and manual control of the network.
4. Initiate periodic testing of emergency communications systems to help ensure that they will be operationally ready when they are needed.
5. Pursue development of more efficient methods of interconnecting diverse networks, and implementation of industry-wide standards to simplify interface considerations.

These initiatives will refine existing network managementcapabilities and enhance the internal management of emergency communications systems.

On a larger scale, the barriers to effective emergency communications are both numerous and complex. Long-standing problems of parochialism, profit motivation and lack of incentive have been compounded by the divestiture of AT&T. The impacts of divestiture have yet to be felt in their entirety, but it is safe to say that they will not help the situation. Adding to the problems is the fact that within the government itself there is no central policy-making body to direct and coordinate the numerous entities whose efforts impact on the telecommunications infrastructure. Every day, the news media report situations that underscore the necessity of maintaining an effective emergency communications capability. The ultimate disaster - nuclear conflict - has been averted thus far, but the possibility is very real. In 1981, President Reagan stated that our national communications system must be made "foolproof" [Ref. 16: p.4], but now, five years later, it most certainly is not foolproof, and in fact may have regressed as a result of divestiture. The requirement is clear. The motivation should be sufficient: "The consequence of failures of communications can be devastating. When communications fail, people die needlessly" [Ref. 1: p.1]. Therefore it is incumbent upon leaders of both government and industry to overcome bureaucratic, economic and political obstacles, and to take full advantage of available resources and advancing technology to develop and implement an emergency communications capability that ensures that vital communications will be available when they are needed most.

APPENDIX A
LIST OF ACRONYMS

ARPA	Advanced Research Projects Agency
AT&T	American Telephone and Telegraph
BOC	Bell Operating Company
CCIS	Common Channel Interoffice Signalling
CCS	Common Channel Signalling
DSN	Defense Switched Network
DTP	Data Transfer Point
EADAS	Engineering Administrative Data Acquisition System
EMP	Electromagnetic Pulse
ESS	Electronic Switching System
HFDF	High Frequency Direction Finding
IEEE	Institute of Electrical and Electronic Engineers
ISDN	Integrated Services Digital Network
ITT	International Telephone and Telegraph
LATA	Local Access and Transport Area
MLPP	Multilevel Precedence Preemption
MTS	Message Telecommunications Service
NCC	Network Control Center
NETS	Nationwide Emergency Telecommunications System
NMC	Network Management Center

NOC	Network Operations Center
NOCS	Network Operations Center System
NS/EP	National Security/Emergency Preparedness
PDN	Public Data Network
PSN	Public Switched Network
PTN	Public Telephone Network
ROC	Regional Operations Center
SPC	Stored-Program Control
SRI	Stanford Research Institute
STP	Signal Transfer Point
WATS	Wide Area Telephone Service

LIST OF REFERENCES

1. Stanford Research Institute International, Final Report: A Review of National Security - Emergency Preparedness Telecommunications Policy, February 1981.

2. Gimpelson, Lester A., "Network Management: Design and Control of Communications Networks", Electrical Communications, Volume 49, Number 1, 1974.

3. Haenschke, D.G. and Ebner, G.C., "Network Management", The Bell System Technical Journal, Volume 62, Number 7, Part 3, September 1983.

4. Wong, Dominic H., "The Future of Network Management", Telecommunication Journal, Volume 53, Number III, March 1984.

5. Westcott, Jil, Burruss, John and Begg, Vivenne, "Automated Network Management", Proceedings of IEEE INFOCOM '85, March 1985.

6. Dzubeck, F.X., "Network Management: A Customer Perspective", Proceedings of the Fifth International Conference on Computer Communications, October 1980.

7. Hyde, P.N. and Wilbur, G.A., "Management of Packet-Switching Networks", Conference Record of GLOBECOM '85 (IEEE Global Telecommunications Conference), December 1985.

8. Jenkins, C.H. and Tor, Z.J., "The Need for Network Management", Telecommunication Journal, Volume 51, Number II, February 1984.

9. Bressler, R.D. and Haverty, J., "Computers in Communication Networks", Telecommunications (North American Edition), January 1986.

10. Mocenigo, J.M. and Tow, D.M., "Managing a network that won't stand still", Bell Laboratories Record, August 1984.

11. Ritchie, A.E. and Tuomenoksa, L.S., "No.4 ESS: System Objectives and Organization", The Bell System Technical Journal, Volume 56, Number 7, September 1977.

12. Browne, Thomas E., Ewin, James C. and O'Reilly, Gerard P., "No.5 ESS - versatile, flexible, forward-looking", Bell Laboratories Record, Volume 59, Number 9, November 1981.

13. Johnson, Jerry W., Kennedy, James C. and Warner, Jack C., "No.5 ESS - serving the present, serving the future", Bell Laboratories Record, Volume 59, Number 10, December 1981.

14. Miller, P.R. and Wallace, R.E., "Common Channel Interoffice Signalling: Signalling Network", The Bell System Technical Journal, Volume 57, Number 2, February 1978.

15. Greene, T.V., Haenschke, D.G., Hornbach, B.H. and Johnson, C.E., "Network Management and Traffic Administration", The Bell System Technical Journal, Volume 56, Number 7, September 1977.

16. Bolling, George H., AT&T: The Aftermath of Antitrust - Preserving Positive Command and Control, National Defense University, 1983.

17. Foree, Stephen C., Secure Transmission of Sensitive Information via the Nationwide Emergency Transmission System (NETS), M.S. Thesis, Naval Postgraduate School, Monterey, California, March 1985.

18. Bartz, W.S. and Patterson, R.W., "National Network Management", The Bell System Technical Journal, Volume 62, Number 7, Part 3, September 1983.

19. Haenschke, D.G., Kettler, D.A. and Oberer, E., "Network Management and Congestion in the U.S. Telecommunications Network", IEEE Transactions on Communications, Volume COM-29, Number 4, April 1981.

20. Sevcik, Peter J., Williams, Graeme J. and Hitson, Bruce L., "Defense Data Network Survivability", Conference Record of EASCON '82 (15th Annual Electronics and Aerospace Systems Conference), September 1982.

21. Oaks, B.G. and Logan, S.R., "Defense Switched Network: Survivability through Proliferation", Conference Record of EASCON '82 (15th Annual Electronics and Aerospace Systems Conference), September 1982.

22. Schmidt, R. and Cronin, J.K., Wartime Reconfiguration of the Public Telephone Network, BDM Corporation, Mclean, Virginia, April 1980.

23. Lomax, John B. and Rubin, Darryl E., Final Report: New Concepts in Survivable Communications Networks, SRI International, Menlo Park, California, July 1981.

BIBLIOGRAPHY

Allers, J.E., Hamilton, S.T. and Kukla, J.A., "The No.5 ESS Switching System: Robust and ready for changes", Bell Laboratories Record, Volume 61, Number 5, May/June 1983.

Carestia, P.D. and Patterson, R.W., "Enhanced software helps managers keep network traffic moving", Bell Laboratories Record, Volume 61, Number 4, April 1983.

Cole, Leo J. and Ryder, Keith D., "The Information System: An Implementation of Network Management in a large SNA network", Conference Record: GLOBECOM '83 (IEEE Global Telecommunications Conference 1983), Volume 2, 1983.

Defense Nuclear Agency, Wartime Reconfiguration of the Public Telephone Network, Final Report, April 1980.

Department of the Navy, Navy Telecommunications System Architecture Study, Final Report, Volume I, May 1974.

Foree, Stephen C., Secure Transmission of Sensitive Information via the Nationwide Emergency Telecommunications System (NETS), M.S. Thesis, Naval Postgraduate School, Monterey, California, March 1985.

Gilkinson, F.M., Corkovic, S.S. and Kennedy, J.A., "Monitoring and Management Systems for DATAROUTE", National Telecommunications Conference Record, 1981.

Haenschke, Detlev G. and Ebner, George C., "Network Management", The Bell System Technical Journal, Volume 62, Number 7, Part 3, September 1983.

Haenschke, Detlev G., Kettler, D.A. and Oberer, E., "Network Management and Congestion in the U.S. Telecommunications Network", IEEE Transactions on Communications, Volume COM-29, Number 4, April 1981.

Hart, Larry, "Network Management - a user perspective", Telecommunications (North American Edition), Volume 18, Number 7, July 1984.

Hedge, Kenneth, "ATC Olympic Network", Telecommunications (North American Edition), Volume 18, Number 7, July 1984.

Horgan, John, "Safeguarding the National Security", IEEE Spectrum, Volume 22, Number 11, November 1985.

Hyde, P.N. and Wilbur, G.A., "Management of Packet-Switching Networks",

Conference Record of GLOBECOM '85 (IEEE Global Telecommunications Conference 1985), December 1985.

Jenkins, C.H. and Tor, Z.J., "The Need for Network Management", Telecommunication Journal, Volume 51, Number II, February 1984.

Johnson, Jerry, W., Kennedy, James C. and Warner, Jack C., "No.5 ESS - serving the present, serving the future", Bell Laboratories Record, Volume 59, Number 10, December 1981.

Kasperek, Gabriel, "Comparing various network management schemes", Data Communications, July 1985.

Lyon, D., "Network Control: A View from the DCE", Proceedings of the Fifth International Conference on Computer Communications, October 1980.

McKenzie, A.A., Cosell, B.P., McQuillan, J.M. and Thorpe, M.J., "The Network Control Center for the ARPA Network", Computer Networking, IEEE Press, 1976.

Miller, P.R. and Wallace, R.E., "Common Channel Interoffice Signalling", The Bell System Technical Journal, Volume 57, Number 2, February 1978.

Mocenigo, J.M. and Tow, D.M., "Managing a network that won't stand still", Bell Laboratories Record, August 1984.

Reed, Terry, "Operating and managing a commercial worldwide network", Computer Communications, Volume 8, Number 3, June 1985.

Ritchie, A.E. and Tuomenoksa, L.S., "No.4 ESS: System Objectives and Organization", The Bell System Technical Journal, Volume 56, Number 7, September 1977.

Santos, P.J., Chalstrom, H.B., Linn, J. and Herman, J.G., "Architecture of a Network Monitoring, Control and Management System", Proceedings of the Fifth International Conference on Computer Communications, October 1980.

Slate, Edward L. and Popko, John A., "The Next Five Years in Communications", Telecommunications (North American Edition), Volume 20, Number 1, January 1986.

Stanford Research Institute International, Final Report: A Review of National Security - Emergency Preparedness Telecommunications Policy, February 1981.

Stach, Jerrold F., "Expert systems find a new place in data networks", Data Communications, November 1985.

Walker, Charles, J., "Network Management in the post-divestiture era", Data Communications, February 1984.

Westcott, Jil, Burruss, John and Begg, Vivienne, "Automated Network Management", Proceedings of IEEE INFOCOM '85, March 1985.

Wong, Dominic H., "The future of network management", Telecommunication Journal, Volume 53, Number III, March 1984.

INITIAL DISTRIBUTION LIST

No.		Copies
1.	Superintendent, Code 54LP Attn: Prof. J. LaPatra Naval Postgraduate School Monterey, California 93943-5000	1
2.	Superintendent, Code 54MO Attn: Prof. D. Moses Naval Postgraduate School Monterey, California 93943-5000	1
3.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
4.	Commander, Naval Security Group Command Code: G30 (Attn: LT R.L. DeLorey Jr.) 3801 Nebraska Avenue NW Washington, D.C. 20390-5210	2
5.	Mr. Ken Boheim NCS/PP 8th Street & S. Courthouse Road Arlington, Virginia, 22204	1
6.	Mr. Edward M. Cain NCS/PP 8th Street & S. Courthouse Road Arlington, Virginia 22204	1
7.	Dr. Bruce Barrow NCS/PP 8th Street & S. Courthouse Road Arlington, Virginia 22204	1
8.	COL William Schooler NCS/EP 8th Street & S. Courthouse Road Arlington, Virginia 22204	3
9.	Mr. Norman Douglas NCS/EP 8th Street & S. Courthouse Road Arlington, Virginia 22204	3
10.	LTC Tom Cindric (JDSSC) Defense Communications Agency Code 662 Washington, D.C. 20305	1
11.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2